# TRANSACTIONS USING A RE-PROGRAMMABLE DATA CARD

## FIELD OF THE INVENTION

**[0001]** The present invention relates generally to storing electronic transaction data for conducting transactions and more particularly to programming a card with data and erasing the same data from the card.

## BACKGROUND

**[0002]** Technology is rapidly progressing to permit information to be stored conveniently on portable instruments, such as transaction cards, to facilitate a variety of non-cash transactions. However, many of the uses for such cards require a different magnetic transaction card for the transaction. These cards usually have a particular type of transaction data encoded into a magnetic stripe. As a result, an individual may be required to carry numerous transaction cards, such as general use credit cards, e.g. Visa®, Mastercard®, American Express®, etc., mono-line cards (i.e. vendor-specific credit cards), automatic teller machine (ATM) cards, as well as cards for club memberships, discounts, point accumulations, insurance information, telephone calls, and many more types of transaction cards.

**[0003]** Multi-purpose transaction cards exist which carry much data required for the defined number of card functions. However, these data-carrying multi-purpose cards create security risks if the card is lost or stolen. The convenient pocket size of these cards allows them to be easily forgotten at the point of sale during a transaction. The value of a card data is compromised until its misuse is discovered.

**[0004]** The cards usually contain a user's personal data and/or carry the codes required to access such personal data stored on an external database, such as a user's financial account. Although the card may utilize some security measures, e.g. password protection, the data still may be exposed to the risk of hackers, and others maliciously gaining access to the personal data. Moreover, these data-carrying cards are highly susceptible to damage. For example, data on magnetic cards may easily become erased due to the effects of magnets on a user's possession.

**[0005]** Where a card is lost, stolen or damaged, it is inconvenient to replenish the data. Typically, new data must be established and the previous data cancelled for each of the card's functions. The more types of functions supported by the card, the more data that must be changed or regenerated for a card.

**[0006]** Some cards may have data replenished or loaded by a card retailer's terminal or other device dedicated to a particular transaction provider. The data that is installed onto the card is limited to data pertaining to that transaction provider or the transaction types to which the provider is involved, such as telephone services or a mono-line card. Therefore, these devices do not provide a user with the freedom to choose data for various types of transactions from a consolidated option list.

**[0007]** Efforts to create multi-purpose transaction cards have also been thwarted by the need for the card to be compatible with a growing number of different devices that read the card data. One category of card that permits a variety of card functions is referred to as a smart card. The typical smart card includes an embedded microprocessor, or the like, and uses processing circuitry for data storage and interacting with a transaction data reader, such as an ATM or merchant terminal. Often, a keyboard or other control panel is

provided on the face of the card to input data into the card. Still, this type of card has limited compatibility with existing and future systems that have different operating systems for which the card was designed. Moreover, the smart card usually includes complicated and expensive components, which may include an integrated chip, power supply, magnetic control circuit, inductor, memory circuitry, LCD display, etc.

**[0008]** In general, the shortcomings of the currently available electronic transaction cards include inability to work with a variety of devices. Furthermore, previous transaction cards are either closed-ended in the number of functionalities it may perform or are programmable but encompass complicated components.

## SUMMARY

**[0009]** The present invention provides a method for performing a transaction, whereby a user-specific data for a transaction type is selected from a plurality of user-specific data for more than one transaction type. The selected data is loaded from a personal data device and onto a transaction card where it is carried without the transaction card needing to employ processing circuitry. The transaction card is presented to a reader device, which retrieves the selected data. At any point after loading of the selected data onto the card, the data may be erased from the card. Typically, erasing occurs after the transaction is complete.

**[0010]** The personal data device may be any computer or intelligent device. Often the personal data device is a portable apparatus that has additional extra-transactional functions as well as operations for transactions, such as a mobile telephone, PDA, etc. The personal data device may be in communication with several other computer devices or server(s) to gather the transaction data, synchronize databases, receive follow-up information after the selected data is retrieved by a transaction provider, and the like. A plurality of user-specific data may be stored as a data set on the personal data device for a large variety of transaction types. A user may select particular data of the data set by selecting a category in one or a series of option menus.

**[0011]** In one embodiment, the transaction card includes a magnetic recording medium in a data area and the personal data device creates a magnetic flux onto the medium, to produce a data pattern. The magnetic data may be erased through randomization from interfering emissions. The emissions may be from an erasing medium on the transaction card, released from the personal data device, or from other device.

**[0012]** The personal data device loads the data for use during a transaction through a loading port. A transaction card that receives the data may be an external instrument communicating with the loading port, or an internal component of the personal data device to which the loading port writes the data. The data area of a transaction card may have several tracks carrying different data as required by various reader devices. The card may also include a track that has data related to the card and not a particular transaction.

**[0013]** In one embodiment of the personal data device, a reading component function is also included that checks the written data during the loading process. A read head may be included as part of a loading port which writes the data.

## BRIEF DESCRIPTION OF THE DRAWINGS

**[0014]** The present invention is illustrated by way of example that is not intended for limitation, in the figures of the accompanying drawings, in which:

**[0015] Figure 1** is a block diagram one embodiment of a transaction environment in which a re-programmable card may be loaded with data by a personal data device for use with a reader device, in accordance with the teachings presented herein.

**[0016] Figure 2** illustrates one embodiments of a personal data device according to the present invention.

**[0017] Figure 3** illustrates writing and reading operations of a magnetic write head and read head of a personal data device, according to one embodiment of the present invention.

**[0018] Figures 4A to 4B** show various embodiments of a re-programmable transaction card, wherein **Figure 4A** represents one example of a self-erasable card and **Figure 4B** represents a portion of an exemplary two track card, according to the teachings presented herein.

**[0019] Figure 5** is a flow chart depicting one method for conducting a transaction with a user transaction system according to the present invention.

**[0020] Figures 6A and 6B** illustrates an example of user-specific data, wherein **Figure 6A** represents one embodiment of data set and **Figure 6B** represents selected data from the data set.

**[0021] Figure 7** illustrates one embodiments of a personal data device having an internal transaction card component, according to the present invention.

**[0022] Figure 8** is a block diagram of a machine-readable medium storing executable code and/or other data to provide one or a combination of mechanisms for storing and transferring data, in accordance with one embodiment of the present invention.

## [0023] DETAILED DESCRIPTION

**[0024]** A user transaction system is provided that includes a personal data device to transfer selected data for use in exchanges with a transaction provider. Data relating to a particular transaction may be chosen from among a plurality of data for various transactions from a consolidated data set. The personal data device may program a transaction card with the data to be conveyed to a provider's reader device. Where the re-programmable card is employed, the card need only be loaded with the data required for the desire transaction and may be thereafter conveniently erased from the card. Furthermore, the transaction card need only carry data for the period of time that it takes to complete the exchange. In this manner of storing required transaction data, the personal data device serves as an "electronic wallet" and a simplistic and versatile card may optionally be used as a data conveyance vehicle.

**[0025]** The present transaction system may facilitate any transaction that requires user-specific data. Such user-specific data may identify a user or pertain to other information that is special to the user and relevant to a transaction, rather than being applicable to the general population not associated with the user. The user transaction system is highly flexible for operation with endless types of exchanges that utilize such user-specific data. For instance, the transaction may be related to a user's personal funds and involve access to a financial account from a remote terminal. This type of financial account transaction often involves personal funds data, such as credit card account numbers, expiration dates, bank account numbers and amounts available for release, as well as authorization codes associated with the accounts.

**[0026]** Some other transactions include telephone calls or Internet access, wherein the data may be a prepaid value amount, access code, and the like; membership management, wherein the data may be information for tracking of member activity, and the like; healthcare services, wherein the user-specific data may include health records, medical alerts (e.g., allergies), prescriptions, and the like; access control transactions, wherein the data may include an identification or authorization code; purchases at vending machines, wherein the data may be prepaid value, etc. These transactions and data types are listed by way of example. They are not intended to limit the transactions and type of user-specific data for which the transaction system may be applied, according to the present invention.

**[0027]** **Figure 1** illustrates one example of a transaction environment **2** in which a user transaction system **4** and a transaction provider **20** are in communication. The user transaction system **4** has a personal data device **6**, a transaction card **8**, and a server **10**. The transaction provider system has components including a reader device **22** at the point of transaction **24** to read the data from transaction card **8**, and a processing center **26** to manage the transaction request. The transaction provider may include a credit card system, banking system, telephone service provider, health care provider, merchandise retailer, postal service, a variety of other parties that use transaction data for providing transactions, or combinations thereof. In transaction environment **2**, the transaction card **8** is programmed by a personal data device **6** with user-specific data that is subsequently read from the card and may be transmitted through the various components of the transaction provider system **20**. Follow-up information may be sent to the various

components of the user transaction system and/or transaction provider in response to the data exchange.

**[0028]** Although **Figure 1** demonstrates one layout of a transaction environment, the scope of the present invention anticipates that the user transaction system may communicate with any number of transaction provider systems having a variety of components arranged in various fashions with reference to the reader device. In addition, in some embodiments, the personal data device may deliver user-specific data directly to the reader device without employing a transaction card as a data conveyance medium. It is further intended that the user transaction system may include any number of servers, including no servers.

**[0029]** The user-specific data, including a data set or a selected portion from a data set, originates at a data source **12**. There are a wide variety of data sources that may supply the data. The data source may be a computer system that communicates with the personal data device, such as the server **10** or a card clearing house. A local storage device that is separate from the personal data device **6** may also serve as a data source such as a wireless phone, personal digital assistant (PDA), laptop, etc. The data source **2** may be a device dedicated for Internet access, such as an Internet appliance. In addition, the data source may be a removable storage module that is coupled to, e.g. insert into, the personal data device **6**. For example, the data source may be a tape, CD, hard drive, disc or other removable storage medium.

**[0030]** In some embodiments, the data source is a device to relay audio data, such as a telephone, speaker, audio recorder, and the like, where the personal data device may also have voice recognition capabilities. Still in other embodiments, the data source is an input

component of the personal data device, e.g. a keyboard, touch screen, cursor control (such as a mouse or trackball), audio receiver (such as a microphone), etc., where data is inputted directly from a user and into the personal data device.

**[0031]** Typically, the data source is portable or remotely accessible. However, static data sources are also possible, for example, where the personal data device or transaction card receives data prior to being transported to the site of the intended transaction.

**[0032]** The personal data device **6** is any apparatus to transfer selected data for use by a reader device, such as loading selected user-specific data onto the transaction card **8** for use as a conveyance medium or directly loading the data to a transaction provider. The device is useful for storing a plurality of user-specific data associated with than one transaction type and usually numerous transaction types, such as 2 to 100 or more types . Often, the personal data device is portable for convenience in transporting to the point of the transaction, i.e. an intelligent portable device, such as a wireless telephone (e.g. cellular, personal communications services (PCS), etc.), PDA, pager, wearable computer, or other wireless intelligent device. However a fixed device, i.e. not easily movable, is also possible. The device may be a computer system, which may be portable, such as a laptop, pocket computer, etc., or may be stationary, such as a desk top computer, e.g. a personal computer (PC), such as a Macintosh® (from Apple Corporation of Cupertino, California), Windows®-based PC (from Microsoft Corporation of Redmond, Washington), or one of a wide variety of hardware platforms that runs the UNIX operating system or other operating systems. The devices listed are by way of example and are not intended to limit the choice of apparatuses that are or may become available

in the data communications device field that may store and transmit data, as described herein.

**[0033]** Often, the personal data device has capabilities of performing functions not related to the transactions, i.e. extra-transactional tasks, such as non-transactional telephone use, storing and manipulating of general-purpose data, calendaring, receiving information across the Internet, notifying a user of a message, playing audio or video, capturing still images, video and/or audio, etc. In other embodiments, the personal data device is a dedicated device for application solely in the user transaction system according to the present invention.

**[0034]** As shown in **Figure 2**, the personal data device **6** includes a communication interface **50** to receive data from the data source, a storage unit **54** to hold the data, an loading port **56** to transfer the data for use by the transaction provider, e.g. encode the data onto the card or transmitting directly to a transaction provider, and a processor **52** to execute the various data manipulation tasks. Usually, the personal data device also includes a power source **62** and a data presentation unit **60**.

**[0035]** The communication interface **50** is for receiving various data and transaction-related information from a local apparatus, an attached device or component that is internal to the personal data device, remote source, e.g. the server **10**. The communication interface **50** may also deliver data to another user device, for example, to synchronize current data with another computing device.

**[0036]** The data may be received through a variety of communication schemes. Such schemes include use of radio frequency, optical frequency or electrical wire transmissions from a communication source using any of the numerous communication standards used

in the telecommunication industry. For example, communication may be through a network, e.g. an Internet connection, satellite transmission, Ethernet connection and other communication links for transferring the data to the personal data device **6**. A transmission may be made at frequencies appropriate for wireless communication schemes, e.g. infrared, etc.

**[0037]** Personal data device **6** also includes processor **52**, which may represent one or more processors to run an operating system and applications software that controls the operation of other device components. Some exemplary processors are a Motorola® Power PC processor, an Intel Pentium® (or x86) processor, etc. The processor **52** may also be a microprocessor. The processor may be configured to perform multitasking of several processes at the same time.

**[0001]** A bus **58** is usually provided to carry information between system components. The width of the bus determines how much data can be sent between components, such as 8-bit, 16 bit 32 bit, 64 bit (e.g. Peripheral Component Interconnect (PCI) bus), etc. However, is some variations of personal data device, particular components may couple directly to each other or through a dedicated bus for the particular components, rather than connecting through bus **58**.

**[0038]** The storage unit **54** is provided to hold the user-specific data, option menus for display to the user through a presentation unit **62** such as a display (e.g. a liquid crystal display), and other transaction-related data. The storage unit **54** may be any magnetic, optical, magneto-optical, tape, and/or other type of machine-readable medium or device for writing and storing data. For example, the storage unit **54** may be a writeable optical compact disc (e.g. CD ROM, DVD), a disc, tape, random access memory (RAM), such as

dynamic RAM (DRAM) and static Ram (SRAM), etc. The amount of storage required depends on the type and amount of data stored. For example, typical user-specific data for a single credit card is about 2 Kbytes of data. Thus, a personal data device for storing 100 credit card data would have a non-volatile memory of at least 200 Kbytes.

**[0039]** In one embodiment, the personal data device **6** also has a temporary storage unit (not shown) to momentarily store the data prior to the storage unit **54** obtaining the data. In another embodiment, the storage unit **54** is the same as or similar to a memory unit for holding program application(s) for the personal data device, that may be one or a collection of various types of memory used.

**[0040]** Often a non-volatile storage, e.g. electrically erasable program read only memory (EEPROM), Flash memory, or cache, is provided for the operating system and resident software applications. The storage unit may also be a hard drive, either integrated within the system, or external and coupled to the system. The storage unit may also be coupled to other types of multiple storage areas that may be considered as part of the storage unit or separate from the storage unit. These storage units **54** described are by way of example and are not intended to limit the choice of storage that are or may become available in the data storage field, as described herein.

**[0041]** One or more option menus may be provided in the personal data device storage unit **54** to assist a user in selecting user-specific data for a transaction. Alternatively, the option menu may be stored on an external device and the selected user-specific data transferred to the personal data device. The option menu lists categories for a variety of different transaction for the consolidated store of a plurality of user-specific transaction data.

**[0042]** **Figures 3A** and **3B** illustrates one example of user-specific data option menus as may be stored in the storage unit **54** of the personal data device and presented to the user by presentation unit **60**. **Figure 3A** is an exemplary data set in the form of branching trees of the option menus, each having categories that lead to specific transaction data and **Figure 3B** is a selected data from the data set of **Figure 3A**. The data set **100** has an option menu **102**, having the data categories: finance, health and membership. Under a chosen finance category, a type menu **104** has data categories: cards, stock and bank. Further to a card category selection, a card menu **106** has categories: XYZ Retail and Visa. User-specific data list **208** has the account information for the card categories. Often, the option menus are presented to a user for category selection. However, the user-specific data list optionally may not be presented to a user where a category was selected in a preceding option menu. In this case, personal data device associates the selected transaction type with appropriate user-specific data type, rather than having a user select a category from the user-specific data list. Each of the data tree branches may include even further sub-menus and transaction data for the categories. The example shows Visa category as chosen from the data set. The specific transaction data for a chosen category of the data set is the selected user-specific data **110**, as depicted in **Figure 3B**.

**[0043]** The personal data device **6** also has a loading port **56** that is in communication with a transaction card **8**. The loading port records data onto the transaction card. The loading port may be a magnetic write head, a laser, an audio recording head, and other components suitable for conveying data for user by a reader device. In some embodiments, the loading port **56** is a read and write head that either has separate gaps for reading and writing or has a single gap used for both reading and writing purposes. In

other embodiments, the personal data device has a read head that is separate from the loading port **56**.

**[0044]** A read function in the personal data device may be implemented to examine the written data and check for completion and/or accuracy. The personal data device interprets signals generated by the read head through detection of the written data and compares the retrieved data to the selected user specific data. The personal data device may further include and indicator to signal when the written data is complete and/or accurate. The indicator may be a light, sound speakers, an alphanumeric message display, and the like.

**[0045]** In one embodiment, a read head may be positioned after the write head relative to the writing path along the recording medium, e.g. card surface, so that the read head may detect the written data during the recording process. For example, a transaction card may be written to and subsequently read from during a single communication period, e.g. a swipe contact. Similarly, where a combination read/write head is employed, the read gap may be located after the write gap according to the writing path.

**[0046]** In some embodiments, the loading port is an electromagnetic field generator or passive magnetic field module. **Figure 4** illustrates the date examination process with a typical magnetic loading port comprising a write head **150** and a separate read head **152**. The heads **150** and **152** have coils **154** wrapped around the back panel **156** of a core **160**. In the write head **150**, the coils are to create a magnetic field **164**. In another embodiment, the coils may be wrapped around the side panels **158** of the core **160** and core may be any length and have a suitable number of coil windings to produce the desired magnetic flux density. In order to reduce the size of a write/read head to fit into

conveniently into a compact personal data device, the coils may be closely wound along the core panels. For example, the head may be 5-10 mm x 5-10 mm x 5-25 mm. Typically, for a head that operates by swiping with a card, the depth of the head must be greater than the thickness of the card.

**[0047]** Between the panels of the core **160** is a gap **162**. This magnetic field oscillates as it travels along the surface of a magnetic recording medium **170** to saturate the medium and vary the direction of the magnetic field at various points on the recording surface. The result is a magnetic current pattern **172** left on the medium that represents the user-specific data. In this example, the recording medium **170** is moved in a direction from left to right relative to the heads.

**[0048]** The read head **152** is positioned to detect the written data from the recording medium. The read head detects the fields from the resulting magnetic recorded regions to create an output voltage during changes in recorded magnetization. Clock pulses are reconstructed from the data within a clock window **174** and are interpreted using an data encoding algorithm. The read data **176** is compared to the corresponding stored selected data. If the data is the same, then the loading is complete and accurate. Otherwise, the loading is not sufficient for data transfer to a transaction provider.

**[0049]** The personal data device **6** also includes a power source **62**, which may be an internal power supply, such as a battery, or a connection to an external power source. In one embodiment, the personal data device includes a single power supply to accommodate the transaction related functions as well as any extra-transaction operations of the personal data device. In the alternative, the personal data device may have separate

power supplies for transaction function and other operations. In general, a writing function requires greater energy than requirements for reading.

**[0050]** In addition, the personal data device may include various other optional components either related or unrelated to the storage and transfer of transaction data. The personal data device may comprise components for performing extra-transactional tasks, such as a transmitter for alternative communications with other devices, e.g. for connecting with a remote other telephone. In addition, there may also be components for alerting a user of an event, such as an incoming message. The personal data device may further include an interrupt unit to disable and enable extra-transactional tasks, e.g. transmission functions, in coordination with loading data onto the reader device or transaction card, where a card is employed.

**[0051]** The transaction card, as illustrated variously in **Figures 5A and 5B**, is an article that carries a recording material in an information-yielding arrangement. **Figure 5A** shows one embodiment of a transaction card **8** having a main body **200** with at least one data area **202** that includes the recording medium **204**. Permanent indicia (not shown) may also be disposed, e.g. printed, on the card, but such indicia are not necessary for the present user transaction system.

**[0052]** The main body of the card may be made of any convenient material, and usually a polymeric substrate, which may be optionally coated with a transparent layer such as silica or gelatin. The card may be any desired size and shape, and usually pocket size, e.g. from about 50.00 x 80.00 mm to 70.00 x 120.00 mm (usually about 53.98 x 85.60 mm) and between about 0.15 mm to 1.0 mm (usually about 0.76 mm) in thickness. The size of

the recording medium depends, *inter alia*, on the amount of data to be stored, the type of recording material employed, etc.

**[0053]** The data area is oriented on the card in a location that is accessible by a reader device. The card may have one track of data in the data area or several tracks for different purposes, such as 2 to 5 tracks having various data fields positioned in a variety of orders. The data fields may also include a clocking bit at the beginning and/or end of the data.

**[0054]** **Figure 5B** shows one embodiment of a partial transaction card **8** with two types of exemplary tracks **220, 222** in data area **202**. Track one **220** is standardized for the International Air Transport Association (IATA). Track one may sometimes be used by airline companies for securing reservations with a credit card, by credit card companies, etc. The recorded data includes a start sentinel **224**, such as "%" symbol, format code **226** and primary account number **228**, which may have a maximum number of digits, e.g. 19 digits. A name field **230** may have a maximum number of alphanumeric characters, e.g. 26 characters, which is separated from an additional data field **232** by a field separator **234**, such as "^" symbol. The additional data field **232** may contain other discretionary transaction data, such as expiration date, offset, encryption codes, etc. The track one **220** also includes an end sentinel **236**, such as "?" symbol and longitudinal redundancy check **238**. There is a leading field **240** and a trailing field **242** of multiple zeros.

**[0055]** Further to the example in **Figure 5B**, track two **222** is standardized for the American Banking Association, such as a track used by ATM's, credit card checkers, etc. The data includes a start sentinel **224**, such as ";" symbol, primary account number **228**, which may have a maximum number of digits, e.g. 19 digits, a field separator **234**, such as "=" symbol, additional discretionary transaction data **232**, end sentinel **236**, such as

"?" symbol and longitudinal redundancy check **238**. There is a leading field **240** and a trailing field **242** of multiple zeros.

**[0056]** In addition, the transaction card may include a card-specific track for containing discretionary data that is not required by a transaction provider. For example, the card-specific track may contain fields for a card identifier, user statistics, number of times the card had been recorded with transaction data, Internet service provider information, etc. This card-specific data is usually not erased after a transaction. Another track may include a thrift track, which is similar to track one and track two in **Figure 5B**. The track may also be updated, i.e. read and written to, during the transaction, by a reader device. Another track may be for Docutel's proprietary system. Other tracks and data fields may be included as required by various readers and transaction providers.

**[0057]** The recording medium in the data area is any material that permits repetitive programming of data thereto. The recording medium further allows programmed data to be removed from the card, restoring the medium's ability to receive other data. Often, the recording medium permits storing of the data without employing any processing circuitry, as found in many smart cards.

**[0058]** One such recording medium is a magnetic material, such as an oxide magnetic material, deposited on the card surface and recorded by forming a pattern that represents the data. A magnetic material stores data through a coercive force, defined as a force of a magnetic field required to reverse the direction of a magnetic flux. A typical low coercive force card has a magnetic iron oxide media of about 300 to 900 oersted (Oe), and usually 600 Oe, that is embedded in the main body of the card. A higher coercive force card has a coercivity in the range of about 2,750 to 4000 Oe. Often a higher force is achieved by

doping iron oxide magnetic particles with materials that increase magnetic anisotropy, such as cobalt or barium (to produce barium ferrite particles). The ease in which the magnetic material can be changed by an applied magnetic field depends on whether the material is soft and exhibits a smaller magnetic hysteresis or hard and has a larger hysteresis. The magnetic materials may be coated on the card by any convenient procedure, such as application of a plastic binder material.

**[0059]** There are other recording mediums that may be employed on the data area in addition to magnetic mediums, such as optical mediums, audio recording medium, and the like, including combinations thereof. For example, an optical hologram medium, such as a polymer material, on the planar surface of the card may record compressed data into a three-dimensional image. The optical hologram medium may be erased by exposure to a specific frequency of light, which is absorbed by the medium.

**[0060]** One type of audio recording medium is sound (vibration) phonon storage using crystal lattice structures as a recording medium. Suitable recording materials for these anharmonic systems may be based on the phonon spectra and phonon dispersion curves for the materials, such as 3He, 4He and other isotopes. A laser is used as a loading port for photon-gated hole burning onto a conveyance medium, e.g. card, to store multiple bits of data. Hole density on the recording medium may be increased by embedding the data area in a polymer. In one embodiment, electron-photon coupling is employed, where electrons are coupled to the lattice vibration of the recording medium. The recorded data may be erased by exposure to waveforms at a frequency that conflicts with the crystal resonation.

**[0061]** Often, the transaction card is a blank transaction card, which is void of transaction data until the card interacts with the loading port **56** of the personal data device **6**. The data area of the transaction card connects with the personal program device to receive transaction data within the recording medium. Communication with the personal data device may be through a variety of mechanisms. For example, the card may be swiped through the personal data device or otherwise contacted with the loading port of the personal data device, the card placed proximal to the personal data device, etc. Where the data area is a magnetic stripe, the personal data device forces alignment of the encoding material to represent the data.

**[0062]** The recorded data remains temporarily on the transaction card and is erased after programming is complete. As depicted in **Figure 5A**, in one embodiment, an erasing medium **86** is intermixed with the recording medium **84** to randomize the data. In other embodiments, an erasing medium may be located at various locations proximal to the recording medium on the card to exert influence onto the recording medium. The erasing medium may be sized and have a predetermined intensity to automatically erase the data at a certain period of time after encoding of the data. For example, the erasing medium may be designed to delete the data within about 3 to 480 minutes after recording, and more typically 3 minutes to 60 minutes, and even more usually 5 minutes to 15 minutes.Furthermore, erasing of the data may occur by an external stimulus, such as emissions of signals from the personal data device or other device, and the erasing medium need not be included on card, although the erasing medium still may be added.

**[0063]** In addition to the transaction card and personal data device, another element that is often included in the user transaction system according to the present invention is a

server **10**, which may communicate with a transaction provider, personal data device, and/or other user devices. The server **10** may receive transaction-related information from a transaction provider. The server **10** may also receive user-specific data or other information from the personal data device for storage in a database. The server usually retains transaction-related data, such as date of transaction, amount transacted, name of transaction party, type of transaction, service fees, interest charges, periodic statements, etc. in one or more database(s).

**[0064]** The server may analyze a transaction, reconcile the transaction and forward the results to the user. Furthermore, the server may provide follow-up information or other transaction-related information to the transaction provider or to the user, such as transmitting the information to the personal data device or other computer system. During the time of the transaction, the server may immediately provide such transaction or follow-up information to the personal data device "on the fly". For example, when a user wants to conduct a transaction, a user may request account information from the server and receive the answers by the personal data device. Immediately after the transaction, the user may receive on its personal data device confirmation of the transaction and the current balance of the user's account or other personal information relating to and resulting from the transaction.

**[0065]** The transaction provider has various segments that may interact with each other and the user transaction system in providing the intended exchange, depending on the nature of the exchange and the transaction provider. A reader device **22** at the point of the transaction 24, e.g. merchant terminal, reads the user's transaction card. Such a reader device is any one of a wide variety of devices at the point of the transaction for retrieving

user-specific data from a card, including general legacy equipment, hardware dedicated for sensing the transaction card, or other future-developed reader devices.

**[0066]** The transaction provider may include a processing center **26** having various substations across a network that may be useful in processing a transaction such as a sponsoring banking institution, a central hub to manage the system, etc. The processing center may supply authorization for a transaction or pass a request for authorization to the server. The processing center may also interact with a card-issuing center that originated the transaction card.

**[0067]** **Figure 6A** shows one exemplary method of implementing the user transaction system to execute a transaction. The personal data device receives data **300**, which is one or more data sets or selected data, through any of a variety of possible mechanisms, *inter alia*, on the nature of the data source. Input of data from an external data source may be through a telephone request and responsive operator-assisted entry, e.g. by a telephone company, cut and paste from another computer application, transmission over a network, etc. Alternatively, the data may be directly inputted into the personal data device by a user, such as through a keyboard, keypad, audio receiver and configured with voice recognition software, etc.

**[0068]** The user-specific data that is selected relates to a particular intended transaction and is often chosen from a data set stored directly on the personal data device. In the alternative, the data may be selected from a data set on another storage system, such as a server, card clearing house system or local storage device, etc., and the selected data may be transferred to the personal data device.

**[0069]** The selected data may be chosen **302** by a variety of mechanisms, e.g. a user command through a selection of variety of option menus, a user query, a user instruction for a particular user-specific data, automatically with the occurrence of an event, a scheduled time for a particular selection, under direction of another computer or device, or the like. Usually, data selection occurs at or close to the time of the related transaction with the transaction provider. For example, data may be chosen when the user is at or proximal to the point of the transaction reader. In this manner, the card may be programmed by a personal data device "on-the-fly" when a user decides to immediately conduct a transaction.

**[0070]** The personal data device loads the selected data to the card **304** when requested by a user, when the personal data device detects contact with or presence of an external transaction card, or other such triggering events. Loading of selected user-specific data to the transaction card may be through a variety of procedures. The card and personal data device may be moved relative to each other by biomechanical operations, electro-mechanical processes, mechanical maneuvering, gravitational forces, etc. The transfer may require contact between a surface of the card and the personal data device or may take place without contact, e.g. placed at a proximal distance to each other, and through emitting of radiation, light, sound waves, etc.

**[0071]** In general for transfers that involve a moving contact surface, the velocity of the data area relative to the loading port need not be constant to provide a relatively uniform spacing of pulses along the data area. For better loading, the speed of the interaction between the card and loading port may be sustained above a minimum and below a maximum threshold. Often, writing to a card requires a more stringent velocity range

than reading from the card. For example, magnetic writing may require a speed of 5 to 35 iterations per second (ips), whereas reading specifications may be 2 to 60 ips. Where an encoding process has failed, the personal digital device may signal a user of the failure through an indicator.

**[0072]**

Where magnetic encoding process is used, the loading port of the personal data device must exert a force that is compatible with a magnetic medium on the transaction card to alter the material on the card. For example, a magnetic field that may be applied by the personal data device must be large enough to oppose the magnetization of the card material. A hard magnetic material on the card has a larger magnetic hysteresis than a soft magnetic material, and requires a larger field from the personal data device to switch directions. Often, the loading port of the personal data device uses a soft magnetic material to conduct the magnetic flux to the head gap, where it is concentrated and spreads out so that it can magnetize the recording medium on the card. The recording medium on the card is typically a hard magnetic material to permit a more stable magnetic state created by the last application by the loading port.

**[0073]** In one embodiment, data transfer is accompanied by a prior or simultaneous and temporary disabling of extra-transaction activities of the personal data device. For example, the personal data device may include a transmitter for communicating to a remote source, such as a telephone transmitter. This disabling permits the personal data device resources to be directed to the programming of the transaction card. The data transfer may optionally be capable of being aborted if the transmitter becomes enabled during the course of the data loading process. For example, if a user accepts a telephone

call, the data transfer may be interrupted if the process had not completed prior to the device transmitter connecting the call.

**[0074]** The user then presents the data to the reader device, which retrieves the selected data from the transaction card **306**. In one type of method according to the present invention, the reader or other terminal at the point of transfer also requests authorization for the transaction from any substation included in the processing center or from the server. The authorization may be registered at the server, a card clearing-house system, or specific other authorization system. Authorization may be with an authorization code or server code authorization program utility.

**[0075]** The processing center may receive a request for authorization and respond or route it to the server. The processing center may also include various transaction substations that may receive the request and either respond or route the request to the appropriate other substation.

**[0076]** If the server receives the request, it references stored user data such as cumulative transaction financial limitations, merchant discrimination criteria, card load balancing or transfer solutions, etc. Upon receiving the request for authorization, the server may also reference transaction related information, such as merchant discounts; comparative pricing analysis; transaction provider specific details, such as insurance, incentives, cumulative merchant purchase-related discounts, rebates, cash, etc; interest rate loyalty reductions or other incentives; etc. The server may send this information to the personal data device or to the processing center, which may also route the transaction related data to a terminal at the point of transaction.

**[0077]** The data may be conveniently erased from the transaction card **308** at any time after loading and usually after the transaction. Erasing restores the recording medium for future loading of data. In one embodiment where the data is encoded by magnetic patterns, the data is rendered unusable by randomization of the magnetic domain information. The erasure may be by entropy of the magnetic data area through thermodynamics. For example, a magnetic stripe on the card may be exposed to a laser light to scramble the magnetic pattern for the data. In an alternative embodiment, the data may be erased by a magnetic field radiating from the personal data device onto the card. The user may place the card proximal to the personal data device, contact the surfaces or swipe the surfaces in order to erase the data. The personal data device may include an erase control for the user to activate the erase components of the personal data device. The erase control may be an option in a menu, a button, screen pad voice command recognition, or other input device. However, a variety of triggering events may also initiate the invalidation of data. For example, the sending or receiving of follow-up information; a signal that the transaction is complete; authorization-dependent variables, such as authorization time period validity; user-defined personal profile, such as cumulative transaction financial limitation reached; or other events.

**[0078]** Furthermore, the erasure may occur by the card having an erasing medium that automatically interferes with the encoded data. For example a magnetic medium on the card may randomize the magnetic pattern by emitting conflicting electromagnetic radiation. Some erasing magnetic mediums include platinum, palladium, cobalt, ferrous alloys, or other elements that may form a composite film. The erasing medium may be proximal to the data area or mixed into the data area. The flux density and grain size,

inter alia, determine the time it takes for the recording medium to become erased, e.g. randomized. The grains of the erasing medium may be sized to remove the user-specific data over a pre-determined period of time.

**[0079]** The transaction system may provide follow-up information to the user, the transaction provider or a designated third party **310**. The user may select a receiving device to accept the follow-up information. For example, the follow-up information may be sent to a corporate system to track expenses made by an employee user to a personal computer of the user, or to the personal data device. This follow-up information may be sent by a server immediately after a transaction is complete, i.e. real time, by or at any designated point during or after the transaction. In one embodiment, the follow-up information is automatically routed to a transaction provider system for acceptance or to the user's wireless device or computer via e-mail, HTML "rich" message, application specific attachment, such as spreadsheet or finance software, e.g. Quicken, from the card service, card clearing house, or server. In one application, the follow-up information is sent to a designated web site to be reviewed with authorized access.

**[0080]** The follow-up information may be a confirmation of a completed transaction, a balance update, notice of required subsequent tasks by the user, advertisements, etc. In one embodiment, the follow-up information may be any useful information that may send the follow-up information directly to an accounting department to track expenses. The data may be in any convenient format. In one embodiment, the data is formatted to be directly loaded into an application-specific program, such as Excel, Quicken, etc.

**[0081]** After all steps are performed, the method ends **312**. Although **Figure 6A** shows one method of employing the user transaction system, the order of sequence for the steps

may be performed in other reasonable orders. For example, the transaction system may send follow-up data prior to erasing the card data, rather than after the removal of data. Also, the written data may be erased prior to the recorder device retrieving the data and the process ends, as where a user decides to abort the transaction.

**[0082]** Furthermore, optional steps may be added to the procedure. For instance, security mechanisms may be provided for the transaction system. A single transaction authorization security protocol may be included in the personal data device permitting the selected user-specific data loaded on a conveyance medium, e.g. card, to be valid for use in only one transaction. Thereafter, new user-specific data must be loaded onto the card from the personal data device for another transaction. In addition, the transaction system may employ encryption protocols in the personal data device to encrypt the data, server encryption protocols, personal identity number (PIN) or other password protections, etc.

**[0083]** In a particular embodiment of a method for a personal data device to write data onto a card as depicted in the flow chart in **Figure 6B**, the device receives a user-data for various transaction types **350**, stores the data in one or more database, and associates the data with its corresponding transaction type. The personal data device also stores one or more option menus with entries that correspond to the available transaction types. These menus are presented to a user through a display **352**, usually in response to a user command to select transaction data. A particular category in the option menus is chosen which is associated with user-specific data **354**. If the chosen category does not have associated data stored, the user in notified. The user may make another selection or input the associated user-specific data. The selected user-specific data that is associated with the chosen category is located and retrieved from storage **356**.

**[0084]** The selected data is written onto a transaction card according to the methods described above regarding the loading port **358**. As the selected data is being written, the personal data device reads the written data from the transaction card and compares the written data to the stored user-specific data that was selected **360**. If the written data is the same as the stored data, then the writing is considered complete and accurate **362** and the process ends **366**. Otherwise, the user may be notified and the user may either direct the personal data device to rewrite the selected data through a write command, or issue an end command **364**. In other embodiments, the personal data device may default to end where the writing is incomplete or inaccurate.

**[0085]** In alternative embodiments of a user transaction system, the personal data device includes an internal transaction card component having a recording medium in a format that is accessible to a reader device. The transaction card serves in the same capacity and has the same attributes as the external transaction card described above. In one example, a transaction card component may be detachable from the personal data device for use by a reader device and may be reattached after the transaction is completed. The card component may be situated in a compartment of the personal data device, i.e. neutral position, and separated by sliding out, popping out, being pulled from the data device, or other such detaching mechanisms. In another configuration, the card component may remain connected to the personal data device and extend from the compartment in the personal data device as needed for a reader device to access the recorded data therein.

**[0086]** As shown in one embodiment of a personal data device **6** having an integrated transaction card in **Figure 7**, the loading port **56** communicates with the transaction card component **70** during the writing process. The transaction card component **70** relays

written data to a reader device. The loading port **56** writes selected data to the internal card component in a same or similar fashion to writing to an external transaction card, as described above with regards to **Figure 6A**. In one example, the loading port has a moveable component **72** to permit the loading port to automatically travel along the length of the recording medium on the card component during a recording process. The erasing component **74** removes loaded data from the card component **70** at any convenient time. Usually, after a transaction, the card component is placed back to its neutral position and is ready for erasing. In this instance, the erasing procedure is frequently pre-scheduled to occur at a particular time after writing the data or is initiated automatically as the card is replaced into its compartment.

**[0087]** In another alternative embodiment of a user transaction system, a portable personal data device may load selected user-specific data directly to a reader device of a transaction provider, rather than programming an internal or external transaction card or other conveyance instrument. Thus, for a direct transfer system, the personal data device **6,** shown in **Figure 1**, communicates with the reader device **22** and the transaction card **8** is optional. The personal data device projects the selected data to a reader device. The loading port of this personal data device transmits the selected data through a variety of wireless mechanisms, such as optical, radio frequency, audio frequency, and the like. The loading port may comprise an antenna, electromagnetic coupling device, such as antenna, transformer, magnetic induced field device, laser, or LED (e.g. for IR LED), electrical interface, such as a smart card writer, etc.

**[0088]** In still other alternative embodiments of the user transaction system, a portable personal data device according to the present invention includes a read unit for detecting

transaction data on an encoded instrument, such as a check or a note. The read unit may be an optical sensor, magnetic reader, or the like, and may further be the read head in the loading port. The personal data device may communicate the retrieved transaction data to a transaction provider. Communication of this instrument data may be through the personal data device's load port, an Internet interface, telephone transmitter, and other methods of local and remote transfer linking components.

**[0089]** For example of an instrument read transaction, account data may be scanned from a check by the read unit. The personal data device may request and/or the user may input other related data, such as the monetary amount for the transaction. The personal data device may thereafter automatically cash the check by establishing communication, such as a telephone link, with a transaction recipient, such as a bank, merchant, ATM, or other payee. The transaction data, including instrument data and amount, is transferred to the recipient, often through direct transfer methods without a conveyance medium.

**[0090]** In addition, various software components, e.g. applications programs, may be provided within or in communication with the personal data device, that cause the processor or other components to execute the numerous methods employed for storing and transferring data. **Figure 8** is a block diagram of a machine-readable medium storing executable code and/or other data to provide one or a combination of mechanisms to process user-specific data, according to one embodiment of the invention. The machine-readable storage medium **400** represents one or a combination of various types of media/devices for storing machine-readable data, which may include machine-executable code or routines. As such, the machine-readable storage medium **400** could include, but is not limited to one or a combination of a magnetic storage space, magneto-optical storage,

tape, optical storage, dynamic random access memory, static RAM, flash memory, etc. Various subroutines may also be provided. These subroutines may be parts of main routines or added as plug-ins or Active X controls.

**[0091]** The machine readable storage medium **400** is shown having a storage routine **402**, which, when executed, accepts data by a receive data subroutine **404** and stores data through a store subroutine **406**, as described above with reference to the storage unit **54** shown in **Figure 2**.

**[0092]** The medium **400** also has a program card routine **410** used to load data onto a transaction card through several subroutines. The write data subroutine **412** may be executed to load the data onto the card, as described above with regards to the loading port **56** in **Figure 2**. The medium may optionally include a read written data subroutine **414** to examine the data written through subroutine **412**. The read subroutine **414** may be part of the write subroutine **412**, executed consecutively or immediately after the write subroutine.

**[0093]** In addition, the medium **400** may optionally include an erase routine **416** to release signals that interfere with the written data and thereby remove the data from a transaction card.

**[0094]** In addition, other software components may be included, such as an operating system **420**. The software components may be provided in as a series of computer readable instructions that may be embodied as data signals in a carrier wave. When the instructions are executed, they cause a processor to perform the data storage and transfer steps as described. For example, the instructions may cause a processor to receive and store data, to detect a card and load data onto the card. Such instructions may be

presented to the processor by various mechanisms, such as a plug-in, ActiveX control, through use of an applications service provided or a network, etc.

**[0095]** The present invention has been described above in varied detail by reference to particular embodiments and figures. However, these specifics should not be construed as limitations on the scope of the invention, but merely as illustrations of some of the presently preferred embodiments. It is to be further understood that other modifications or substitutions may be made to the described user transaction system as well as methods of its use without departing from the broad scope of the invention. Therefore, the following claims and their legal equivalents should determine the scope of the invention.